National Aeronautics and Space Administration

NASA SAFETY CENTER

SYSTEM FAILURE CASE STUDY

MARCH 2016 VOLUME 9 ISSUE 1

Asynchronicity

The Near Loss of the Apollo-Soyuz Test Project Crew

PROXIMATE CAUSE

- Toxic gas entered the cabin during repressurization for 30 seconds from manual deployment of the drogue parachutes to the disabling of the Reaction Control System.

UNDERLYING ISSUES

- Oxidizer boiloff
- Time-critical manual switching
- Procedure conflict
- Emergency oxygen masks

AFTERMATH

- Astronaut hospitalization.
- Successful completion of the Apollo-Soyuz Test Project and closeout of the Apollo Program.
- Scrutiny of automatic and manual functions for future designs conducted with the understanding that crew error is a possible outcome for all critical functions.

In an extraordinary display of international cooperation during the height of the Cold War between the US and former Soviet Union, television viewers around the globe tuned in July 17, 1975 to witness Apollo-Soyuz Test Project (ASTP) astronauts and cosmonauts shaking hands between their docked, orbiting spacecraft. Following two days of joint experiments, shared meals, and press conferences, the Soyuz crew undocked their spacecraft and landed in Russia July 21. The Apollo crew continued on-board experiments until their July 24 re-entry. During descent, the crew did not activate the Apollo's Earth Landing System (ELS) at the correct altitude. As a result, toxic propellant fumes entered the Command Module (CM) through open cabin pressurization valves before splashdown, threatening the lives of America's first orbital ambassadors.

BACKGROUND

Nominal Apollo ELS Design Change

During descent and re-entry, pyrotechnics devices were utilized to jettison the apex cover (forward heat shield), deploy and release the drogue parachutes, and deploy the main parachutes. The ASTP re-entry procedure required the crew to arm the ELS pyrotechnic buses at an altitude of 50,000 ft. Seconds later, at 30,000 ft, the crew was to manually arm the automatic ELS sequencer by positioning two ELS switches to "LOGIC" and "AUTO." After main parachute deploy, the crew were to manually start the Reaction Control System (RCS) propellant dump sequence: first close the Cabin Relief Valve, CM RCS Logic to ON, CM Propellants to DUMP, and then CM Propellant to PURGE. At 3,000 ft. manually turn CM Propellant to OFF (terminates Purge) and at 800 ft. Cabin Pressure Relief Valve to CLOSE. This was recognized as a very high task load for such a short time period.

In December 1969, a decision was made to eliminate the crew safety Single-Point Failures (SPFs) on the ELS pushbutton switches by wiring contacts in series on Skylab CMs. In January 1970, the same desicion was made for Apollo 15 and later spacecraft. This allowed pyrotechnic buses to remain armed after CM/Service Module (SM) separation, removing the need to manually arm during the time-critical re-entry sequence.

Once armed, the ELS applied power to baroswitches, which would close at 24,000 ft to activate the ELS relay, disabling Apollo's

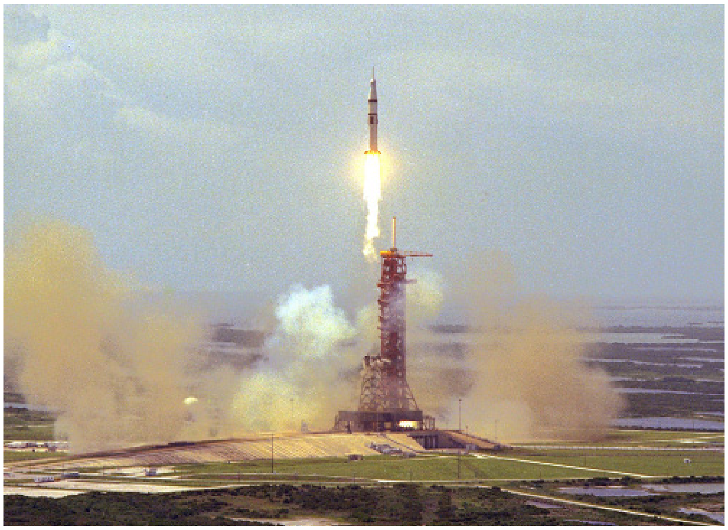

Figure 1. The Apollo crew of the ASTP mission lifting off in a Saturn IB launch vehicle. Source: NASA

RCS and enabling timer relays to release the apex cover and deploy both sets of parachutes sequentially down to 10,000 ft. Manual switches could disable the RCS, which fired toxic nitrogen tetroxide gas, N_2O_4, to stabilize descent until parachute opening, and deploy the parachutes if the redundant automatic system failed to operate.

Crucial to this incident, the spacecraft's cabin pressure release valve opened automatically during descent at 24,000 ft to equalize cabin pressure with ambient pressure outside. The ELS was designed to disable the RCS automatically by that altitude. The entire ELS sequence lasted only 26 seconds in AUTO. At 40,000 ft, if the CM was unstable, the checklist required the crew to select the RCS CMD switch to OFF, APEX COVER JETT pushbutton PUSH. Then, two seconds after the apex cover jettisoned, DROGUE DEPLOY pushbutton PUSH.

What Happened

Prior to flight, engineers explained the wiring design change to the Commander (CDR) and the reason for the current procedure. They tried to convince him to have ELS I AUTO for the Mission Control Center to confirm, before blackout, the parachutes could be deployed automatically. The CDR, who had flown Apollo 10, insisted the original Apollo 10 procedure should be used and they would remember to manually arm the pyrotechnic buses at 50,000 ft and the ELS sequencer at 30,000 ft.

However, during the actual descent, the Command Module Pilot (CMP) armed the ELS pyrotechnic buses approximately 20 seconds late at 37,000 ft. Falling behind the time-critical descent profile, the CDR read the checklist, but the CMP did not acknowledge or arm the two automatic ELS sequencer switches when the Docking Module Pilot (DMP) called them out at 30,000 ft.

As the CM hurtled from 30,000 ft. to 24,000 ft., the CDR stated 24K and realized that the drogue parachutes had not deployed automatically. The DMP said, "Hit your button there." The CMP immediately pushed the guarded APEX COVER JETT pushbutton and then the DROGUE DEPLOY, this jettisoned the apex cover and deployed the drogues at 19,700 ft. and 18,550 ft. At approximately 16,000 ft, the CDR stated he had the Propellants OFF (RCS isolation valves closed). However, the RCS was still enabled because the automatic ELS function had not been armed, and the manual RCS "CMD" (Command) switch had not been thrown to OFF. The CDR then realized the ELS was not in AUTO and switched LOGIC and AUTO (RCS commands disabled) at 9,600 ft and deployed the main parachutes at 7,150 ft.

Closure of the propellant isolation valves allowed the oxidizer trapped between valves and thrusters to boil off. With the cabin pressure relief valve open, reddish-brown N_2O_4 flooded the cabin. Spacecraft control had not been returned to the stabilization and control system minimum-impulse mode at 90,000 ft. (In this control mode, the RCS responded only to manual commands). The gas irritated the crew's skin and eyes and they began coughing — impeding intercom communication within the CM and to ground control.

Upon splashdown, the CM flipped over, suspending the three crewmen upside down in their harnesses. The CMP hung unconscious and the others coughed while the CDR freed himself to retrieve their emergency oxygen masks, which had been stowed

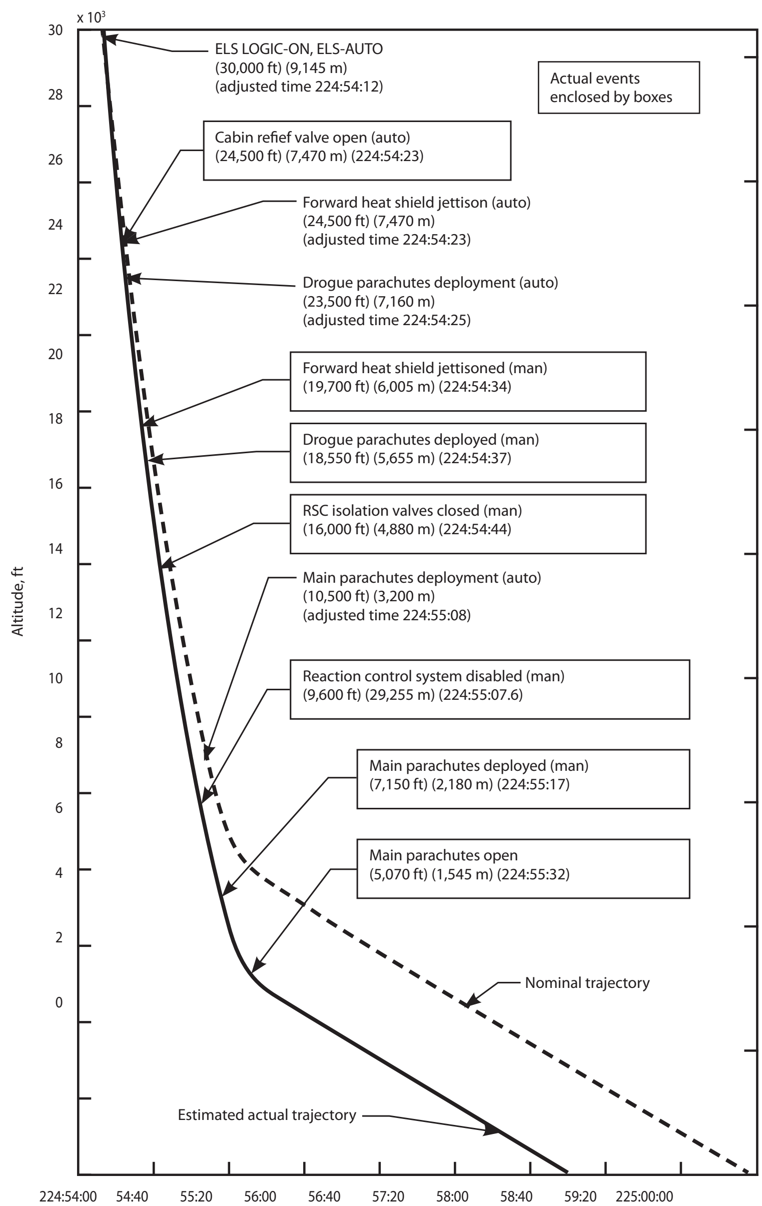

Figure 2. Comparison of actual and nominal ASTP descent sequences. Source: NASA

and were inaccessible during descent. The crew donned masks, and after regaining his senses, the CMP actuated the spacecraft's uprighting system.

The CDR opened the vent valve and the toxic cabin fumes circulated out with the salty, ocean breeze. Divers secured the Apollo craft to a helicopter, which took the crew and spacecraft to the *USS New Orleans.*

Proximate Cause

Toxic gas entered the cabin for 30 seconds from manual deployment of the drogue parachutes to the disabling of the RCS. Crew exposure was estimated to last 4 minutes and 40 seconds.

Underlying Issues

In lieu of relying on the new redundant wiring change, the crew did not follow the Program-approved procedure to arm the pyrotechnic buses at 50,000 ft and to enable the automatic ELS at 30,000 ft. The crew did not follow the advice of Apollo engineers to enable the automatic ELS prior to re-entry communications blackout.

Oxidizer Boiloff

During the 30-second period of high RCS thruster activity, N_2O_4 oxidizer was expelled from the thrusters for a period of 7 seconds. Then, when the CDR closed off the propellant isolation valves, the oxidizer — trapped between the isolation valves and the thruster solenoid valves — began to boil off as the thrusters operated for another 23 seconds (before the RCS was inhibited by the RCS disable relay).

The cabin pressure relief valve opened automatically at 24,500 ft to allow outside air to vent into the cabin to equalize cabin pressure with ambient atmospheric pressure. The valve was located 2 ft downwind of the firing end of one of the positive RCS roll thrusters. Designers had not addressed the potential for the valve to open with the thruster still firing.

N_2O_4 reacts with air to form a variety of nitrogen oxides, principally nitrogen dioxide, NO_2. Although N_2O_4 and NO_2 gases are colorless,

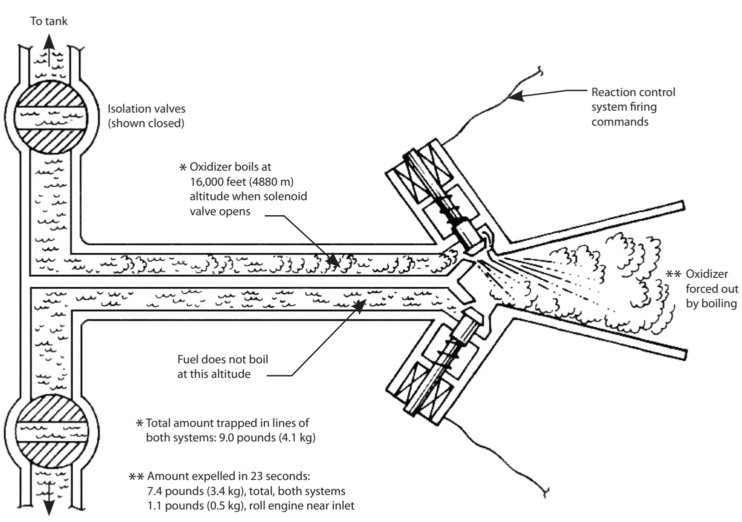

Figure 3. The ASTP oxidizer boiloff process. Source: NASA

Figure 4. The uprighted ASTP CM during recovery in the Pacific Ocean. Source: NASA

the intermediate state of nitrogen trioxide, N_2O_3, varies from yellow to reddish-brown as air concentrations increase. The CDR stated that he observed a dark reddish-brown cloud suddenly occupying his entire field of view lasting between 20 to 30 seconds and containing clearly discernable suspended particles or droplets. The crewmen were exposed to an average concentration of NO_2 of approximately 250 parts per million over a period of 4 minutes and 40 seconds (with a peak exposure of approximately 700 parts per million), from closure of the RCS isolation valves until they were able to equip emergency oxygen masks approximately 1 minute after landing.

Medical findings support exposure to high levels of oxidizer products, but found that the crew was not exposed to other toxic compounds such as monomethyl hydrazine.

Time-Critical Manual Switching

The ELS was designed to operate automatically, with manual backup. This design approach eliminated the need for manual switching in case of a time-critical ascent abort. But from T-minus zero until reaching 24,000 ft, ELS logic switch failure with the ELS in AUTO was rated as a Criticality 1 SPF because the baroswitches would remain closed until the CM climbed above 24,000 ft. Above that altitude, since the ELS sequencer baroswitch design was redundant (both series and parallel), ELS logic switch failure would not prematurely activate the ELS.

Different Apollo crews flew the ELS in several modes. The crews of Apollo 7, 12, and, 13 chose to fly in AUTO, but crews of Apollo 8 and 9 did not trust the original SPF baroswitch wiring and flew with the ELS in MANUAL. Apollo 10 launched in AUTO, then flew MANUAL after T+30 seconds; Apollo 11 launched in MANUAL and switched to AUTO after escape tower jettison. The January, 1970, Apollo Program-approved change rewired the ELS pushbutton switch contacts to prevent premature operation if the pyrotechnic buses were armed. The change was effective for Apollo 15 and subsequent flights; but the crew procedure to leave the pyrotechnic buses armed after CM/SM separation was made for the Apollo 16 and subsequent missions.

In other words, time-critical manual switching had been employed on several early Apollo flights to protect against an SPF. However, for Apollo 15 and subsequent flights, the sequencer pyrotechnic buses were redesigned to be safely armed prior to re-entry. Yet, the ASTP crew did not trust the redundant ELS wiring and reverted to the Apollo 10 procedure of arming the buses at 50,000 ft manually during their descent (Apollo crews had flown in AUTO or MANUAL regardless of mission procedure until Apollo 15). However, in this case, the decision to prioritize manual procedures over designed automation nearly proved fatal:

1. Spacecraft control was not returned to the proper mode at 90,000 ft.
2. The pyrotechnic buses were not armed at 50,000 ft.
3. The RCS was not disabled "RCS CMD-OFF" at 24,000 ft.
4. The two switches that arm the ELS sequencer were thrown 55 seconds after the intended 30,000-ft mark.

The Apollo Soyuz Mission Anomaly Report concluded that timely performance of any one of the missed functions would have prevented the entry of toxic gases.

Procedure Conflict

RCS CMD-OFF was listed on the CMP's Panel 1 entry cue card as a normal function rather than being flagged with asterisks denoting a backup function as on the checklist. The DMP's entry cue card on Panel 3 was simplified 6 months prior to launch; most manual backup tasks, including RCS CMD-OFF, were omitted. In training, the RCS CMD switch was never turned off unless the CDR did so when manual backup procedures were used. If there was breakdown of communication due to noise or when the backup manual procedures were required, the CMP used the Panel 1 entry cue card. The capability for the DMP to take over or assist the real-time callout of entry procedures during the time-critical earth landing sequence was restricted by the major change to the Panel 3 landing cue card, which deleted the RCS CMD-OFF and other backup manual tasks. The conflict between the cue card and checklist concerning RCS CMD-OFF may have contributed to the RCS not being manually disabled when the CMP switched to cue card backup procedures.

The CMP stated in a post-mission interview that he threw the proper switches as the CDR read steps from the entry checklist.

Emergency Oxygen Masks

The emergency oxygen masks were designed for use as a backup to the oxygen breathing circuit during unsuited operations on orbit in case of smoke or contamination in the cabin, but were stowed during descent. The crew's exposure may have been minimized had the masks been accessible from the restrained crew position during entry and landing.

Aftermath

The Apollo crew recovered during a two-week period in Honolulu. The ASTP astronauts and cosmonauts then conducted goodwill tours in the US and USSR. Warm public receptions in both countries meant that the descent incident had not detracted from the overall success of ASTP. As the last Apollo-era mission, ASTP closed the Apollo Program out on a good note.

Relevance to NASA

After the rewire of the ELS switches, the system was designed to be armed for automatic operation of the ELS function prior to communication blackout. The baroswitches were series and parallel redundant and no longer SPFs. Crew training and involvement in design changes are important to build knowledge, trust and contingency readiness.

The ASTP re-entry incident sent a message: increasingly complex spacecraft design drove the need for crew comprehension of the systems behind the latest procedures — and no discretion to revert to older procedures. In August 1978, the director of operations for the new Space Shuttle Program wrote that astronauts "would not be permitted to either change or deviate from well-established procedures," a new NASA requirement. Already rigorous training added a dimension of standardization. Today, that tradition continues on board the International Space Station.

Further, the importance of redundant design in critical electrical controls was demonstrated. The effects of a failure to follow a time-critical procedure in a tightly coupled system should be addressed in training and documentation such that the operator understands system function in both nominal and off-nominal states. Then, if the automatic behavior does not match the operator's expectation of correct function, manual backups can be used — if time allows — to maintain safety and mission success.

References

Apollo-Soyuz Mission Anomaly Report No. 1: Toxic Gas Entered Cabin During Landing Sequence. National Aeronautics and Space Administration, Lyndon B. Johnson Space Center. Houston, Texas. December, 1975.

Ezell, Edward Clinton and Linda Neuman Ezell. The Partnership: A History of the Apollo-Soyuz Test Project. The NASA History Series. NASA SP-4209. NASA Scientific and Technical Information Office, Washington D.C. Published 1978. Web version (updated): November 18, 2005. http://www.hq.nasa.gov/office/pao/History/SP-4209/cover.htm

Redmond, Charles. The Flight of Apollo-Soyuz. http://history.nasa.gov/apollo/apsoyhist.html accessed October 8, 2015.

SYSTEM FAILURE CASE STUDY

NSC

NASA SAFETY CENTER

Responsible NASA Official: Steve Lilley steve.k.lilley@nasa.gov

Special thanks to Gary Johnson for his contributions to this study.